

JUL 24 2007

Application Number 10/656,751
Amendment dated July 24, 2007
Responsive to Office Action mailed April 24, 2007

REMARKS

This amendment is responsive to the Office Action dated April 24, 2007. Applicant has amended claims 1, 18, 35, and 47. Claims 1-64 are pending, with claims 9-17, 26-34, 42-46, and 55-64 being withdrawn.

Claim Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 1, 3-5, 7-8, 18-22, 24-25, 47-51, and 53-54 under 35 U.S.C. § 103(a) as being unpatentable over England (US 6,757,824) in view of Dexter Kozen, "Efficient Code Certification," Dept. of Comp. Sci., Cornell Univ., Jan. 8, 1998, hereinafter "Kozen." The Examiner rejected claims 2, 23, and 52 under 35 U.S.C. § 103(a) as being unpatentable over England in view of Kozen, and further in view of Rudoff et al. (US 6,263,378, "Rudoff"). The Examiner also rejected claims 35-41 under 35 U.S.C. § 103(a) as being unpatentable over England in view of Kozen and in further view of Ong (US 2004/0177258). Applicant respectfully traverses the rejection to the extent such rejections may be considered applicable to the claims as amended. The applied references fail to teach, suggest, or disclose the inventions defined by Applicant's claims.

For example, Applicant's independent claim 18 are directed to a device (e.g., a computer) having an interface to retrieve boot code from a peripheral device, a control unit to verify security of the boot code associated with the peripheral device, and a memory module that stores the boot code retrieved from the peripheral device. According to claim 18, the control unit executes the boot code based on a result of the security check.

In the Office Action, the Examiner primarily cited England, col. 7, lines 18-46 in support of the rejection of claim 1. In general, England describes using a client computer to download content from a content provider, wherein the content provider verifies that the client computer is using a properly registered operating system. *See* England, Abstract. According to England, this verification is to ensure that the operating system has not been stolen, i.e. that the operating system is legitimate. *See* England, col. 1, ll. 52-63.

The portion of England cited by the Examiner describes the verification of the identity of the operating system in detail. The client computer 200 requests content from content provider 220; content provider 220 must validate that client computer 200 is using a legitimate operating

Application Number 10/656,751
Amendment dated July 24, 2007
Responsive to Office Action mailed April 24, 2007

system, therefore content provider 220 requests certificates that identify the operating system of client computer 200 as a legitimate copy. *See* England, col. 7, l. 19–col. 8, l. 12. Client computer 200 retrieves the certificates from an independent boot authority, which content provider 220 trusts. England, col. 7, ll. 22–25; col. 7, ll. 42–45. Client computer 200 sends these certificates to content provider 220. England, col. 7, ll. 60–67. Content provider 220 then sends the requested download to client computer 200 pursuant to the certificate check, and client computer 200 in turn may execute the downloaded content. England, col. 8, ll. 3–5.

Therefore England fails to teach, suggest, or disclose a device in which a control unit retrieves boot code from a peripheral device and then verifies the security of that boot code. England also fails to teach a device in which a control unit executes the boot code retrieved from the peripheral based on a result of the security check required by Applicant's claim 18.

Instead, England teaches that a content provider verifies legitimacy of an identity of operating system components of a client computer in response to a request for content, and the client computer executes the content. This is quite different from retrieving and verifying the boot code from a peripheral device.

Moreover, claim 18 specifically requires performing a security check on the boot code in a accordance with a certificate that describes operation of the boot code. England performs in a manner which Applicant recognizes as prior art, namely ensuring that the software comes from a trusted source. *See* Applicant's specification, ¶ [0006] (describing, as background, limitations of prior art methods of merely verifying whether the code originates from a trusted source). In no way does England utilize a certificate that that describes operation of the boot code. Consequently, the method of England fails to account for a situation in which a legitimate copy of the operating system has become infected with a virus. For example, even in England the content provider may only verify the legitimacy of the operating system, but the content provider is unable to verify security of the operating system. Thus, for many reasons, England fails to teach, suggest, or disclose an interface to retrieve boot code from a peripheral device and a control unit to verify security of the boot code of the peripheral device.

Kozen likewise fails to overcome the deficiencies of England; namely, Kozen fails to teach, suggest, or disclose a control unit to verify security of a boot code associated with a peripheral device. Like England, Kozen addresses only the situation where software is

Application Number 10/656,751
Amendment dated July 24, 2007
Responsive to Office Action mailed April 24, 2007

downloaded from a foreign source. Likewise, neither Rudoff nor Ong overcome the deficiencies of England. Therefore, the combination of references cited by the Office fail to establish prima facie obviousness of Applicant's claimed invention.

Although the above discussion has focused on independent claim 18, similar arguments may be made with respect to independent claims 1, 35, and 47. For example, claim 1 requires retrieving boot code from a peripheral device and verifying security of the boot code associated with the peripheral device. Claim 1 also requires that the certificate that describes operation of the boot code. Similarly, claim 47 requires instructions to retrieve boot code from a peripheral device and to verify security of the boot code associated with the peripheral device. Independent claim 35 as amended requires a computer having an interface to retrieve the boot code and the certificate from the peripheral device, a second memory module and a control unit, wherein the control unit uses the interface to retrieve the boot code and the certificate from the peripheral device and executes a verification module that verifies security of the boot code.

Claim 35 as amended further requires a peripheral device having a memory module, wherein the memory module stores a boot code and a certificate. In the Office Action, the Examiner cited Ong as teaching a peripheral device having a memory module, wherein the memory module stores a boot code and a certificate. However, Ong describes a device "for authenticating [a] user via physicalization of user credentials at a hardware device." Ong, ¶ [0015] (emphasis added). Ong therefore fails to teach, suggest, or disclose a peripheral device having a memory device, wherein the memory module stores a boot code and a certificate and a computer having a control unit, wherein the control unit uses the interface to retrieve the boot code and executes a verification module that verifies security of the boot code. Although Applicant does not acquiesce as to whether one of ordinary skill in the art would have had a reason to combine the England, Kozen, and Ong references, even if one had combined the references, one would still not have met the requirements of Applicant's claim 35.

The claims dependent on independent claims 1, 18, 35, and 47, namely claims 2-8, 19-25, 36-41, and 48-52, incorporate all of the limitations of the respective base claims, and therefore are patentable for at least the reasons expressed above. In light of the shortcomings of England, even in view of Kozen or in further view of Rudoff or Ong, with respect to the independent claims, Applicant reserves comment with respect to the dependent claims. For at

JUL 24 2007

Application Number 10/656,751
Amendment dated July 24, 2007
Responsive to Office Action mailed April 24, 2007

least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims 1-25, 35-41, and 47-52 under 35 U.S.C. § 103(a). Applicant respectfully requests withdrawal of this rejection.

CONCLUSION

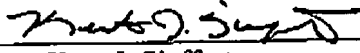
All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

By:

July 24, 2007

SHUMAKER & SIEFFERT, P.A.
1625 Radio Drive, Suite 300
Woodbury, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102


Name: Kent J. Sieffert
Reg. No.: 41,312